REINERSCT

cyberJack® RFID universal

User manual

Content

1 Foreword 1

2 Device description 2

2.1 How to unpack and install the reader 2

3 The functions of your chip card reader 3

3.1 Device Manager 3
3.2 The function of secure PIN input 7
3.3 How to display revision 9
3.4 Module Management 11
3.5 How to switch off the RFID field 13
3.6 Integration of the cyberJack chip card reader in applications 13

4 How to install the hardware on the PC 14

4.1 How to install drivers under Windows 14
4.2 How to install the software components 14
4.3 How to install drivers under Linux 17
4.3.1 Linux.deb 17
Description for ubuntu 17
Description for debian 18
4.3.2 Linux.rpm 18
4.4 Driver installation under Mac 19
4.4.1 Mac OS X 19

5 Safety notes 22

6 Support 23

7 Technical references 24

7.1 LED functions 24
7.2 Technical operating environment 25
7.3 Security functions 25
7.4 Regulatory Notes 27

8 Declaration of Conformity 28

8.1 cyberJack RFID universal 28

Index 29

1 Foreword

Dear customer,

Thank you for choosing an RFID chip card reader from the cyber***Jack***® **RFID** family of **REINER SCT**. The device was developed and manufactured with great care in Germany and will therefore support you reliably for many years. In the following we want to briefly inform you about the most important fields of application of the cyber***Jack***® **RFID** chip card reader.

What is RFID?

The Radio-Frequency Identification (RFID) Technology enables contactless communication between a chip card and a reading device. The number of systems which support this radio technology is constantly rising. For example: contactless payments using money or credit cards, time recording, access control, animal identification, merchandise and inventory management. Besides employee ID cards and the electronic passport, the new german ID card also communicates with the reading device via RFID.

This state-of-the-art technology simplifies chip-card handling and enables them to be used in many new applications.

We wish you great success with your new device

REINER SCT
Reiner Kartengeräte GmbH & Co. KG
Goethestraße 14
78120 Furtwangen
Germany

www.reiner-sct.com

V1.00 25.10.2012

2 Device description

2.1 How to unpack and install the reader

Unpacking

The packaging contains[1)]:

- cyber***Jack***® **RFID universal**
- Stand Base
- USB cable
- Brief instructions on how to install the device
- Driver CD

1)
Depending on the version and the source of supply, the contents may vary or there are additional components in the packaging.

How to install cyber*Jack*® RFID universal

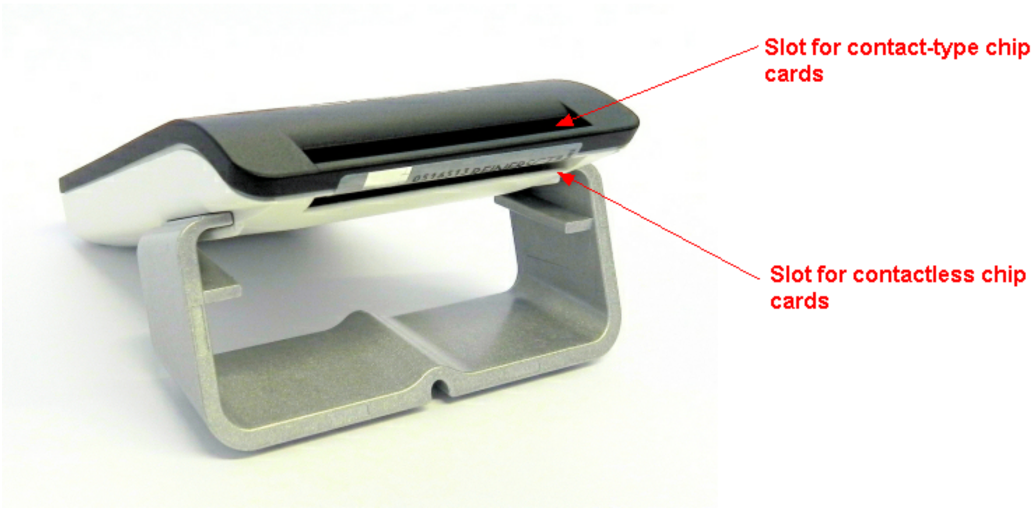
Please remove the device and the USB cable supplied with it from the packaging and plug the USB cable into the socket on the rear of your cyber***Jack***® **RFID universal** . The arrow on the small plug must be visible to you. Then insert the USB cable into the cable duct in such manner that the cable is conducted to the rear or side. If you conduct the cable to the rear you can also use the other cable duct in the foot. Install the device in such manner that you always have all operating elements within your field of vision and you can easily operate the keyboard.

Please pay attention that metallic or metallised conducting or aqueous materials below, or close to, the chip card reader may influence the chip card reader's characteristics for physical reasons. Therefore you must avoid operating the device close to such materials.

This device is intended for use in an office or home environment.

How to handle the cards

The cyber***Jack***® **RFID universal** can be used to read out both contact-type and contactless chip cards. Two separate slots for cards are provided for the purpose. The front slot is for the contact-type chip cards and the rear slot for the contactless chip cards.



3 The functions of your chip card reader

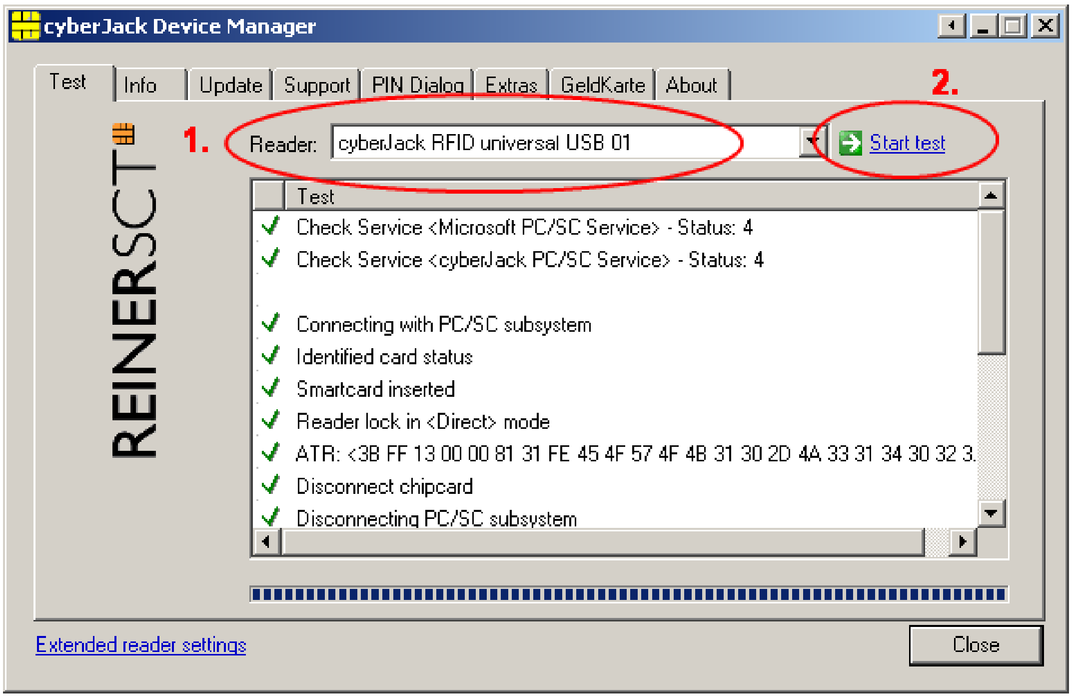
3.1 Device Manager

The cyberJack Device Manager is only available for the Windows operating system at the moment.

After the restart please start the cyberJack Device Manager program, function test in the Start menu under Start > Programs > REINER SCT cyberJack. When the Device Manager starts a registration dialog is displayed to you. We recommend that you make use of the opportunity to register because you will then always be informed about new developments which offer you even more benefit from your cyber***Jack***® .

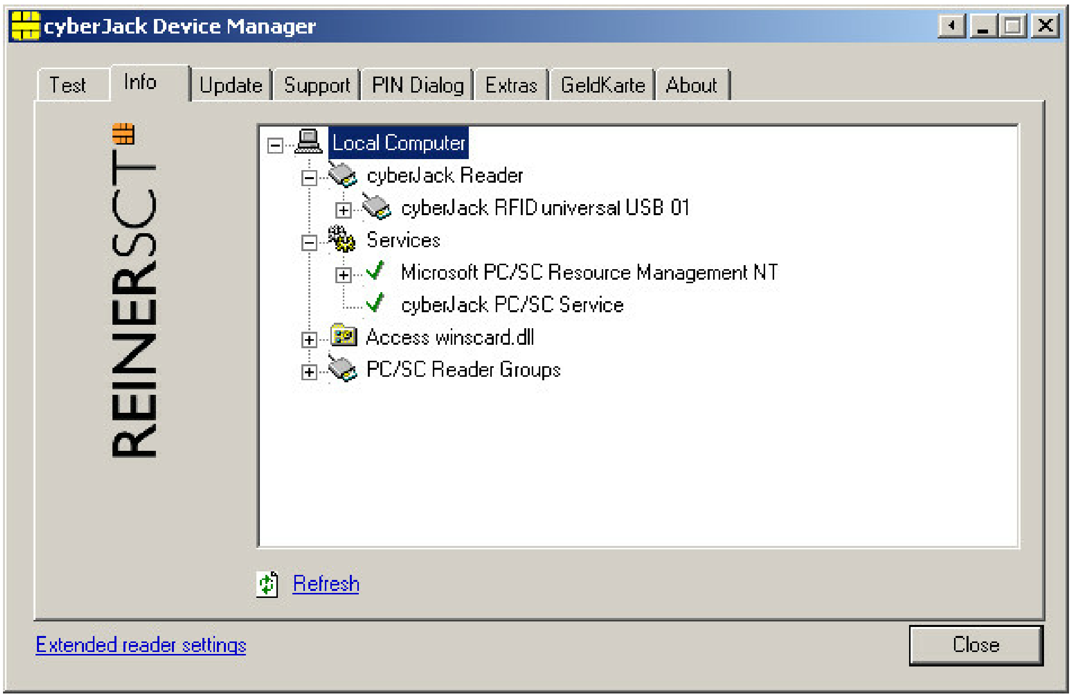
Test tab

If you have connected multiple chip card readers you can select the relevant chip card reader under (1). Take a random chip card (cash card, telephone card, insurance card etc.) and insert it completely into the slit (half the length of the card disappears into the device) of the cyber***Jack***® as indicated by the symbol on the device and the [Start Test] button (2). Various tests are performed, thus checking if the cyber***Jack*** was installed correctly. If a fault occurs during the test you will find help under the Support tab. Here you can immediately establish a connection to the Online Test wizard and send an error log to our Support.



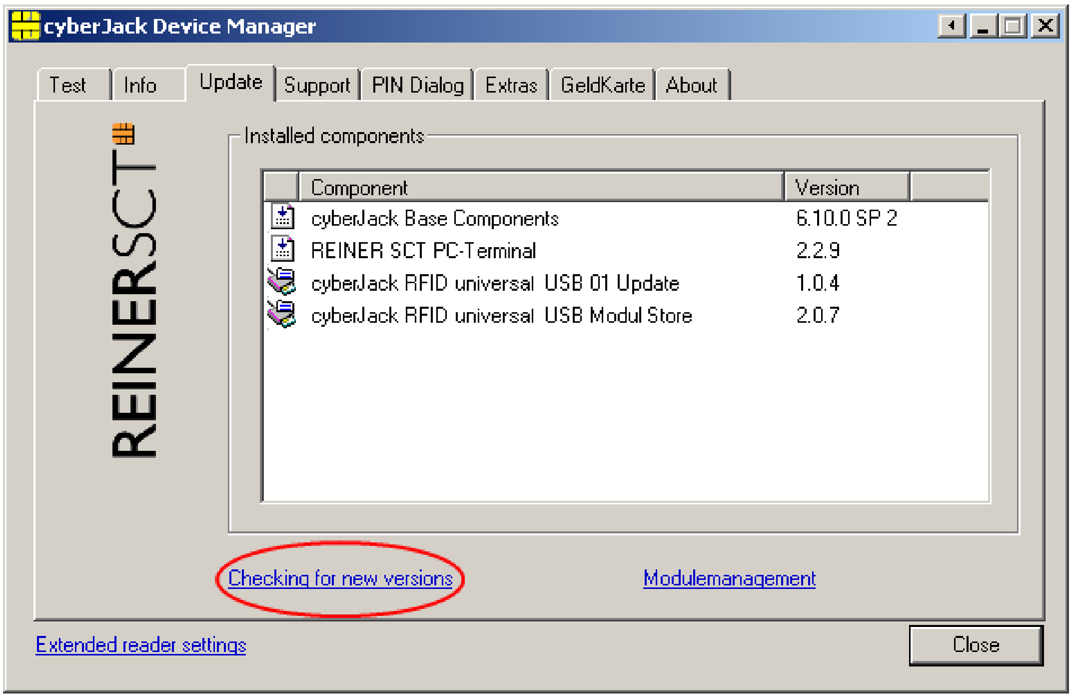
Info tab

In the Info tab various operating and configuration states of the chip card reader and the components belonging thereto are displayed.



Update tab

In Update you can check if you have the up-to-date driver status and firmware for the cyber***Jack***® **RFID universal** . By activating the link **Check for new versions** your Internet browser is started and a connection to the REINER SCT Download server established. If your browser is not conveniently linked to an RDT connection, please start it manually before checking for new versions. If there are new versions, you can update your system directly. For this purpose follow the menu navigation.

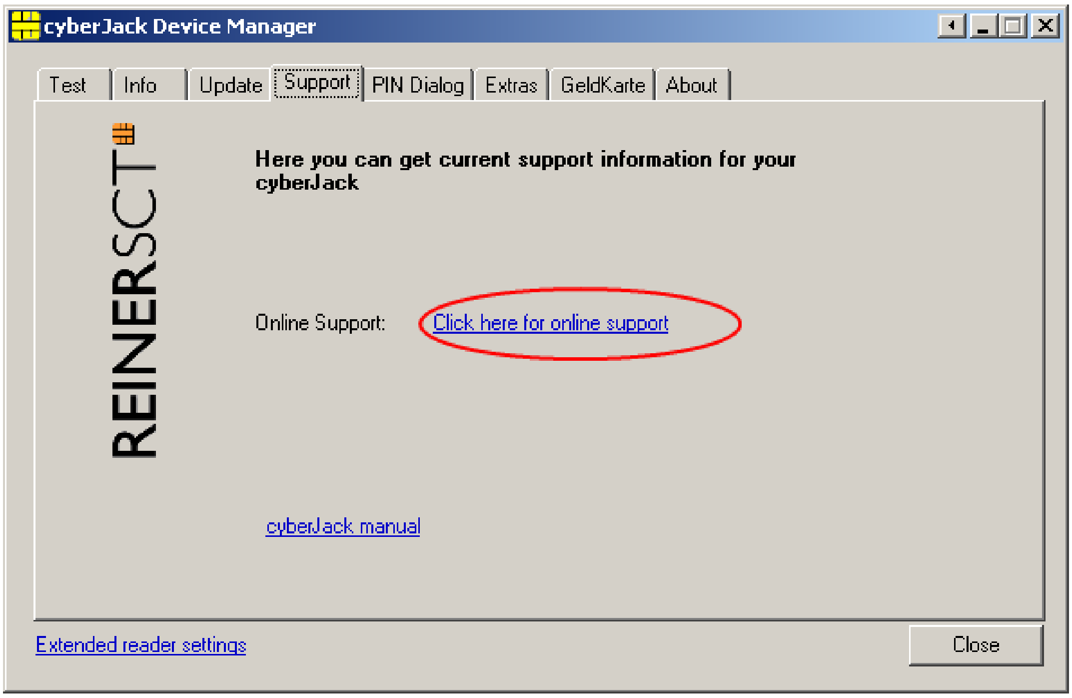


Thereafter you can update the module management of your existing modules and the firmware of the chip card reader.

Further information is available in the chapter Secure firmware download. 11

Support tab

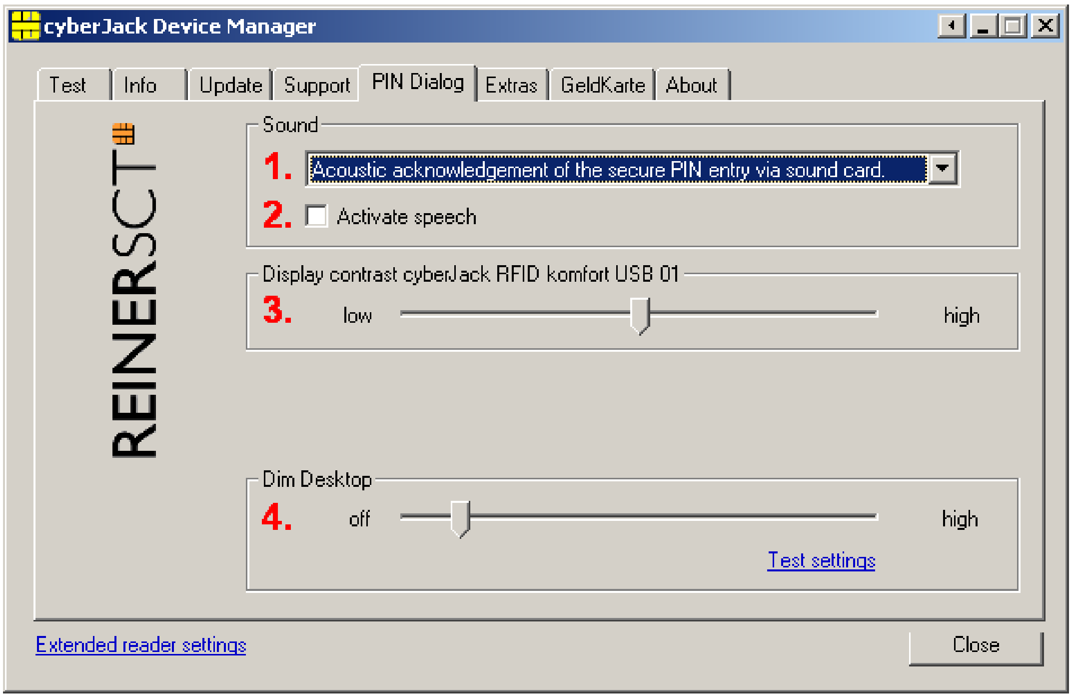
Via Support you can contact the REINER SCT Support directly. For this purpose your current cyber ***Jack***® installation data and some important information regarding your PC configuration are determined and sent to REINER SCT by e-mail. A member of our Support team will then contact you by e-mail or telephone.



PIN Dialog tab

The PIN dialog contains special functions which can be activated and certain special configurations made. Some of them are only needed on very rare occasions; therefore in case of doubt the factory configuration should be retained.

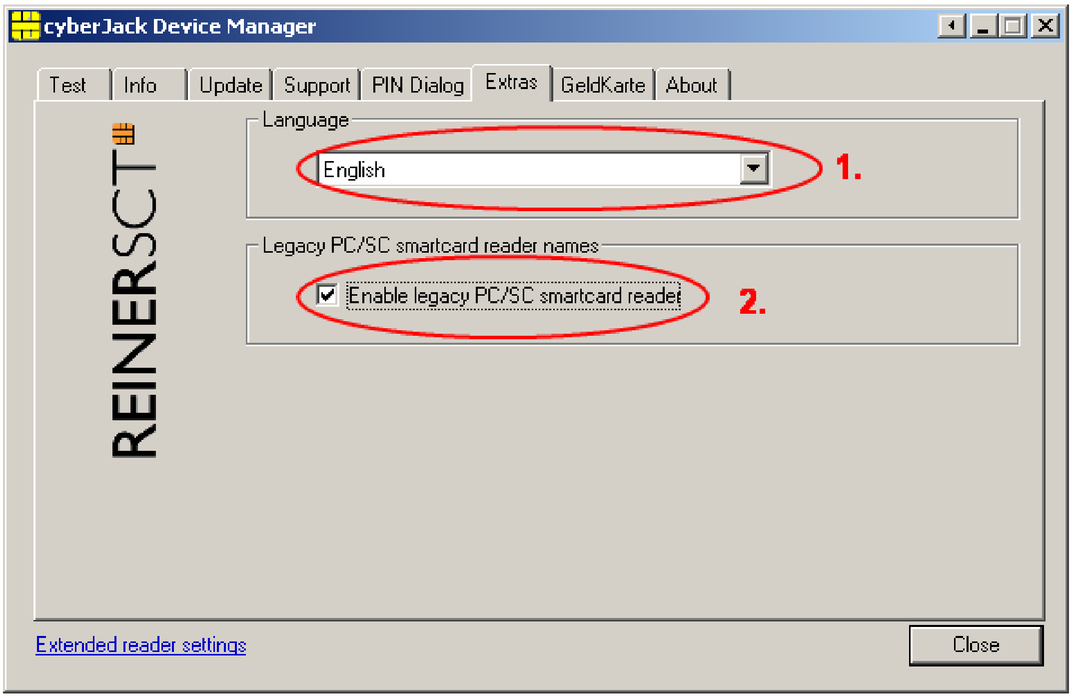
Acoustic settings
(1) Here you can choose whether pressing the key for the PIN input should generate a sound.
(2) Tick here and the request for the PIN is given acoustically by a friendly voice.
(3) Here you can adjust the display contrast of the chip card reader and hence obtain the optimal setting for reading out the chip card reader display.
(4) During PIN input you can darken the desktop by means of slide control. You can test the degree of the setting by means of the **Test Setting button** .



Extras tab

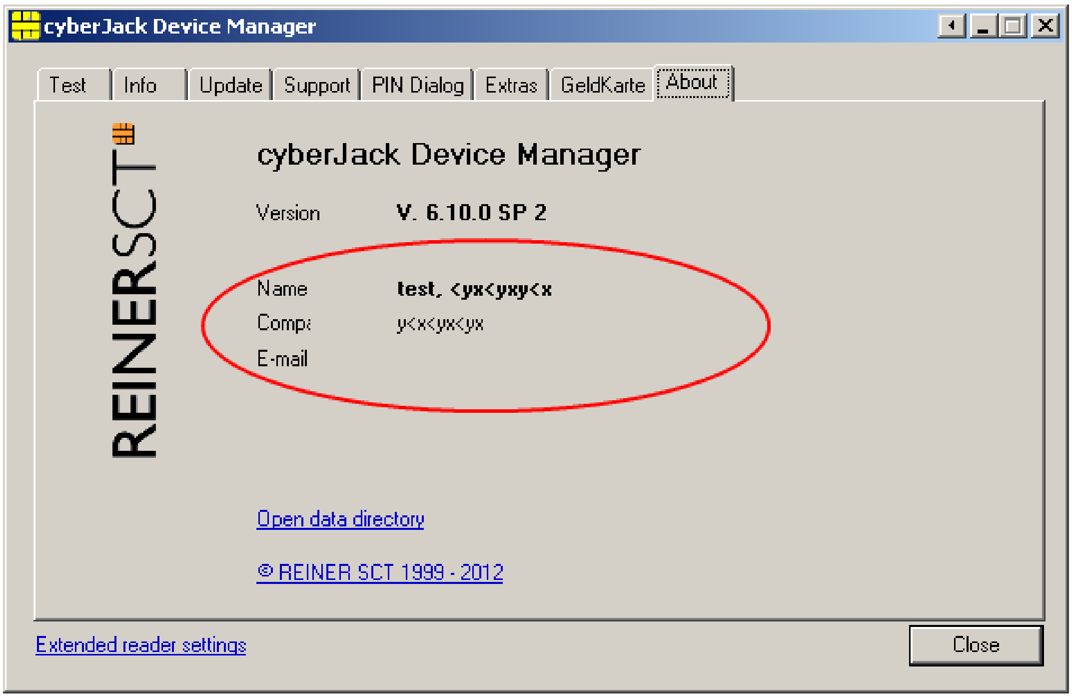
Here you can select the language for the Device Manager (1).

In the case of some signature applications it may occur that our chip card readers are not identified. Then the old PS/SC reader names must be activated (2).



About tab

Here you can find the registration information you have given as well as a direct link to the home page of REINER SCT where you can find information about new products. If you have not yet registered, you can do it here whenever you like.



3.2 The function of secure PIN input

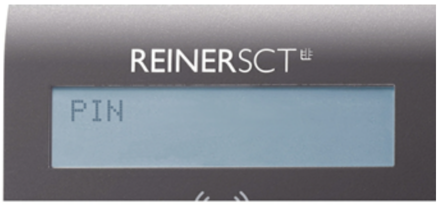
The secure PIN input function serves to keep your PIN code in a secure environment. Various hacker attacks had already aimed at spying out the PIN. The attackers benefit from the fact that the PC represents an insecure environment in which keyboard inputs can easily be recorded and sent via the Internet. Secure input of the PIN is controlled by the PC application. Most programs in the fields of home banking and electronic signature support this function.

The PIN may only be input if the flashing yellow LED signalises the presence of a secure channel between the keyboard and the cyberJack® RFID universal. In addition the green Duo LED lights up when a contact-type chip card is accessed, or the blue Duo LED lights up when a contactless chip card is accessed. Please pay attentionthat nobody is watching you while you are inputting the PIN and conceal the PIN!

Display and LED indicator during PIN input

If a secure PIN input with a contact-type chip card is started by the application the yellow LED flashes and the green Duo-LED lights up. If a secure PIN input with a contactless chip card is started by the application the yellow LED flashes and the blue Duo-LED lights up. The PIN can then be input within the specified time.The time between the input of two PIN numerals is 5 seconds, whereby 5 seconds are available for each PIN numeral. The PIN dialog is shown on the display of the chip card reader. The `*` character here stand for a feedback for a single press of the key. The PIN numerals themselves do not leave the chip card reader and cannot be read off it at any time.

The following display screens appear on the chip card reader if a secure PIN input is necessary.

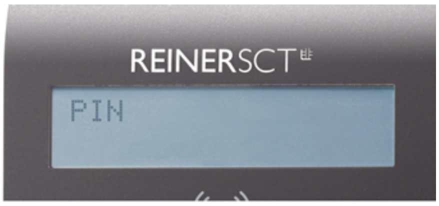


Request Secure PIN

Request Signature PIN

Secure changing of the PIN

In order to change the PIN in secure mode the current PIN must first be input. Thereafter the new PIN is input twice. Each PIN input is acknowledged by pressing the [OK key]. The following display screens appear.



1. Input current PIN

2. Input new PIN

3. Repeat new PIN

Secure changing of the PIN is not supported by all chip cards. In case of doubt please contact the card issuer (bank, trust-centre etc.).

The meaning of the PIN pad keys

0 - 9	Input the PIN numerals
OK	Acknowledgement of transactions, e.g. of the input PIN
C	To abort the PIN input
CLR	Deletes the PIN
@	Indication of revision
UP arrow key	Function application-specific
DOWN arrow key	Function application-specific

Each time a push of a key is processed by the chip card reader a short acoustic signal is output. This acoustic signal is the same for all keys.

Security function for secure PIN input

Secure PIN input is one of the most important security functions of a chip card reader from security class 2 upwards. Secure PIN input is feasible with both a contact-type and a contactless chip card. To ensure that the PIN is not stored in the chip card reader the hardware and the software of the chip card reader have been subjected to strict security-related evaluations. To ensure that the PIN cannot be stored on the inserted chip card, within the "Secure PIN input" mode only commands which can be used for authentication purposes are forwarded to the chip card.

These are exclusively:

- VERIFY
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- RESET RETRY COUNTER

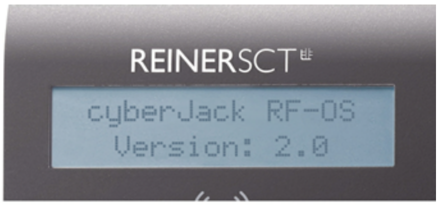
All other commands to the chip card are blocked by the chip card reader.

3.3 How to display revision

There are two ways of displaying the revision of the chip card reader.
When it is inserted into the USB port of the computer or the @ **key** by pressing it on the inserted chip card reader the version and any applications which may be present are shown in the display. While the revision is displayed the yellow LED flashes steadily until the standard operational screen appears. The steady flashing signalises that the text displayed is authentic.

All of the following display screens are examples and may vary depending on the version status.

Sequence of display screens without uploaded application

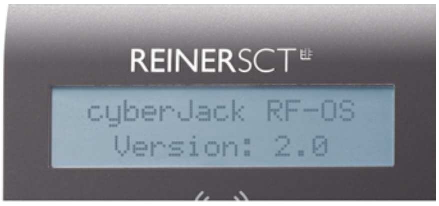


Version screen

**Chip card reader ID screen
(screen shown only if the @ key is pressed)**

Standard screen in chip card reader operation

Sequence of display screens with uploaded application



Version screen

Chip card reader ID screen
(screen shown only if the @ key is pressed)

Screen for the uploaded application
(screen shown only if the @ key is pressed)

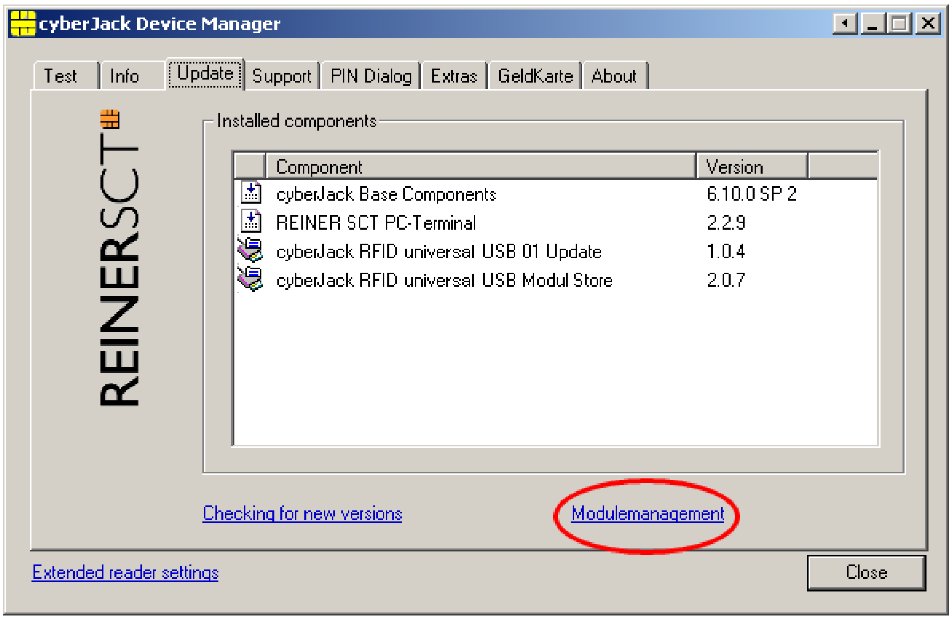
Screen for the revision of the uploaded application
(screen shown only if the @ key is pressed)

Standard screen with chip card reader in operation with uploaded application

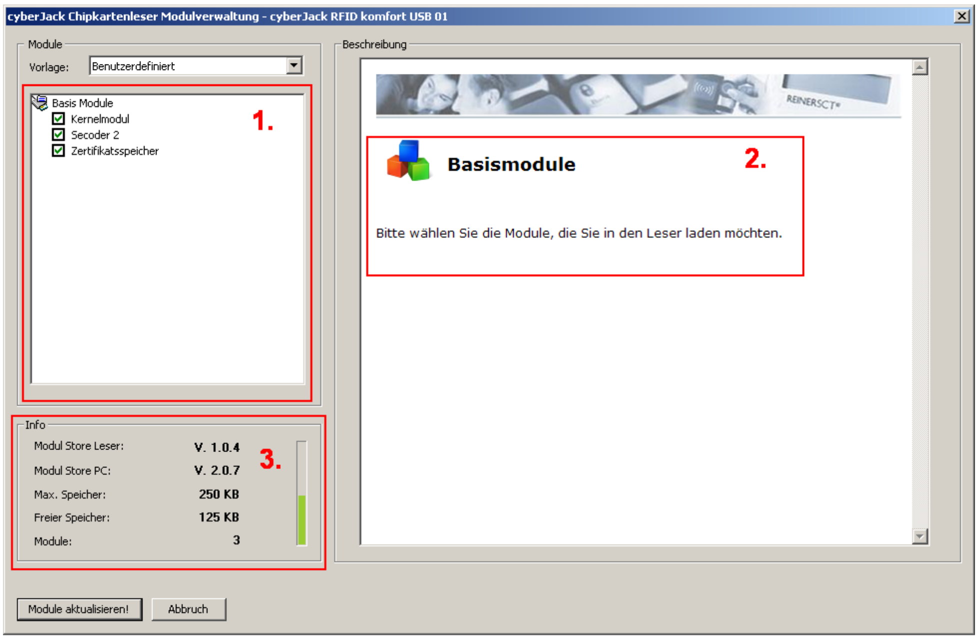
3.4 Module Management

It is possible to add new modules to the chip card reader with the aid of the Device Manager (refer to Device Manager 3 chapter).

These different modules are grouped together in the Module Store. The Module Store is to be found in the Module Management.



To enter the Module Management change to the **Update tab in the Device Manager**. Click on **Module Management**.



The available modules for your chip card reader are to be found on the left-hand side (1). On the right-hand side (2) you will find some explanations about the various modules. In the Info window (3) you obtain information about the storage capacities and version statuses.
The Module Store Reader is the version status of the connected chip card reader. The Module Store PC is the status of the Module Store currently stored on the PC. If necessary, this can be updated via the **Update > Check for new version** tab.

Description of the Module Store downloads

1. Start the Device Manager.
2. Switch to **Update** tab.
3. Click on the **Check for new versions** link (the presence of a new version is checked online on the REINER SCT home page)
4. If necessary, download the new version by clicking on Continue and following the instructions of the InstallShield Wizard.
5. In the **Update** tab click on **Module Management**.
6. **Update modules** .
7. In its display the chip card reader inquires after "Update firmware".
8. After the OK key is pressed the yellow LED flashes briefly during verification of the firmware (signature check).
9. The end of the download is indicated in the Device Manager.

In order to upload new firmware (kernel module) into the chip card reader the check of the origin of the firmware is carried out by the chip card reader itself as an important security function. The chip card reader only accepts firmware which is electronically signed by REINER SCT by means of the RSA method. Each time before uploading new firmware the chip card reader always performs a signature check. It is impossible to store firmware in the chip card reader which has not been electronically signed by REINER SCT. REINER SCT provides only evaluated modules.
It is impossible to update the cyber***Jack***® **RFID universal** to an older version.

Once the new firmware has been activated, the current firmware version can be dispalyed in the chip card reader by means of the Info tab of the Device Manager (after the term Prod.Ref the current firmware version of the chip card reader is displayed). The current firmware version is also displayed directly after the chip card reader is inserted or by pressing the @ key in the display. While the revision number is being displayed the yellow LED flashes.

After a module update, if the display screen shows **"Ready for update"** (refer to chapter 3.3) or after the @ key has been pressed the revision of the application is no longer displayed, the module update must be repeated.

3.5 How to switch off the RFID field

You can deactivate the RFID chip card reader field. This can be useful if, for example, you are using only contact-type cards.

For this purpose you press the UP arrow key. You will see the status of the RFID field in the display.

The RFID field is switched on

The RFID field is switched off

To change the field status press the DOWN arrow key.

Change request

Acknowledge display screen using the OK key.

The RFID is now switched off

3.6 Integration of the cyberJack chip card reader in applications

Electronic Banking

As a rule, integrating the chip card reader into the home banking application is very simple. Many programs already recognise the cyber***Jack***® automatically. Some applications require that the CT-API-DLL be specified. This is the ctrsct32.dll for all devices of the cyber***Jack***® family and is contained in the Windows system directory.

Electronic signature

Software packages for the application of the electronic signature frequently use the PC/SC interface. The drivers are already incorporated in the operating system.

Cash Card

Information on potential uses of the cash card are to be found on the Internet at www.reiner-sct.com/geldkarte-shops.

4 How to install the hardware on the PC

4.1 How to install drivers under Windows

This RFID chip card reader is currently supported by the following operating systems: Windows 2000 / Windows XP 32 bits, Windows Vista 32/64 bits / Windows 7 32/64 bits, and Windows Server 2003 – 2008 R2 32/64 bits.

The cyber***Jack***® **RFID universal** with USB connection must not be connected to the USB port of the computer until the driver has been installed and the computer has been rebooted.
The cyber***Jack***® **RFID universal** is connected to the USB port of your computer or to a USB hub.

Please proceed as follows:
1. First install the drivers as described in "How to install the software components" 14.
2. Then plug the USB plug of the cyber***Jack***® **RFID universal** into the corresponding USB port of your PC. Should the USB ports of your computer be occupied already, you need an active USB hub with an independent power supply.
3. Within a few seconds your system shows that a new system component has been found and the device driver belonging to it is being installed.

How to proceed with the driver installation for the different operating system is to be found in the following chapters:

4.2 How to install the software components

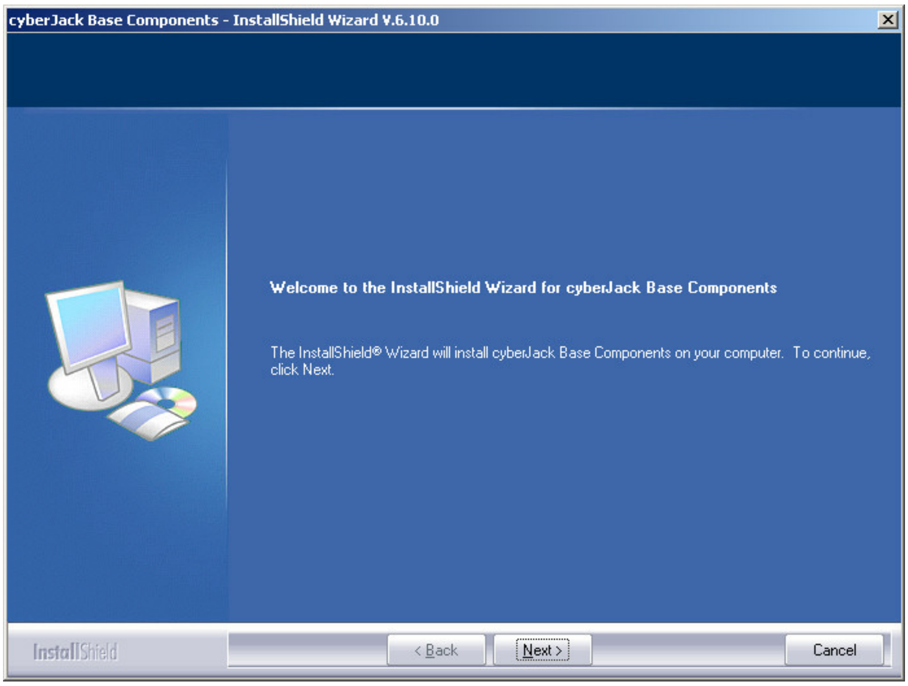
Insert the cyber ***Jack***® driver CD into the CD drive of your computer. With the Installation Manager which then starts you can install various software components for the cyber***Jack***® chip card reader family conveniently and simply. If your system does not support the Autostart function, you can start the installation by double-clicking on the setup.exe file which is on your CD.

Owing to the fast development in computer technology it can happen that the drivers on the enclosed CD are not always up to date. After installation please use the "Check for new versions" function (see 6.1 Device Manager) and, if necessary, perform the proposed update. Thus your installation is guaranteed to be up to date.

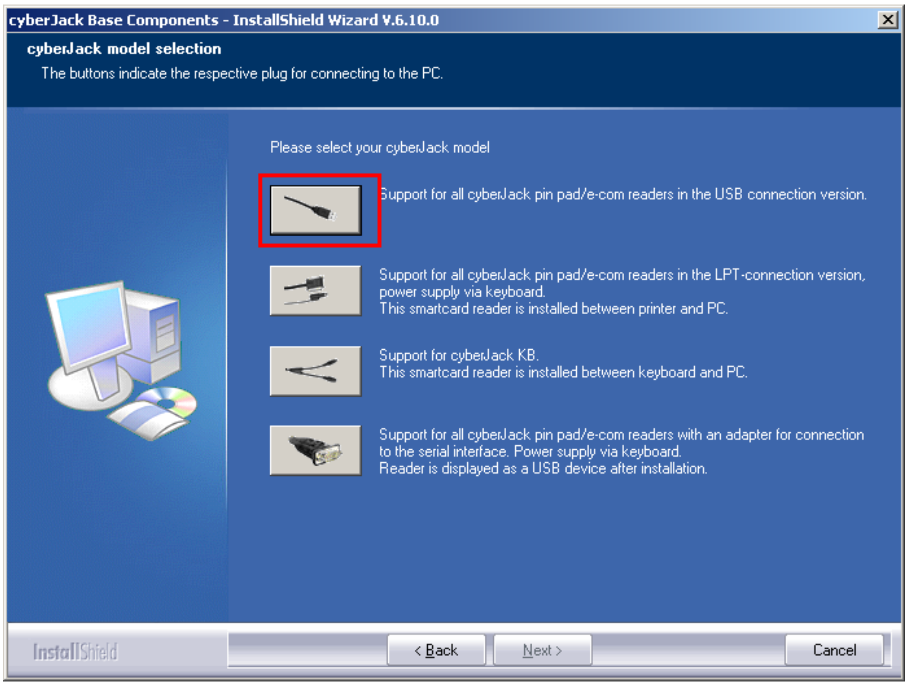
The installation cyber***Jack***® Base Components is absolutely necessary for operating the cyber***Jack***® **RFID universal** chip card reader. They contain the system drivers. Moreover the Device Manager is installed with the device test, driver update and Online support functions.

Press the button, [Start installation] in order to begin with the installtion of selected components. If multiple software components are installed via the Installation Manager, a requisite reboot does not take place until after the last of the components has been installed.

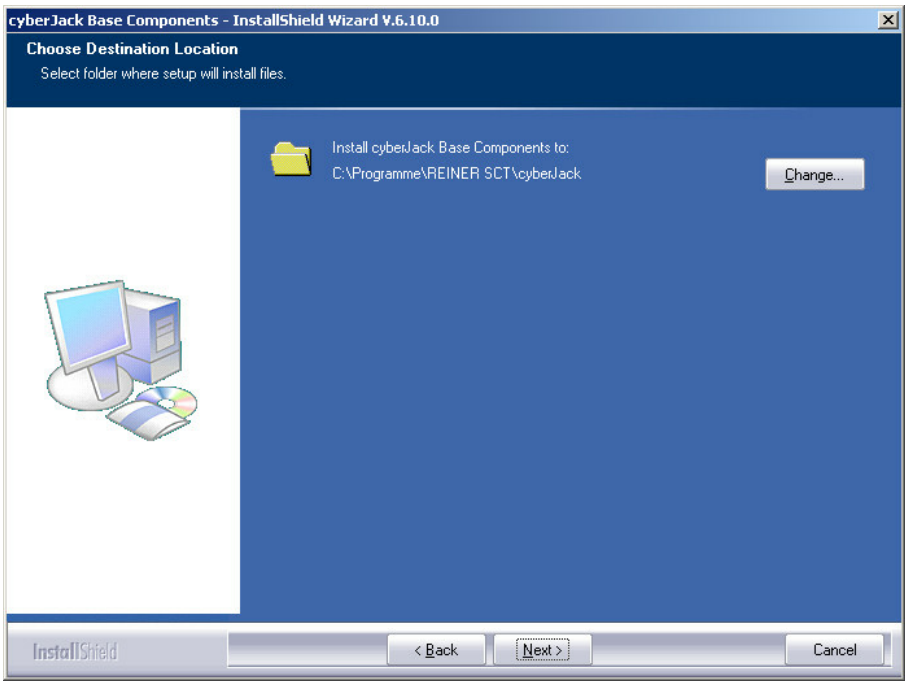
If you want to install the cyber *Jack*® Base Components under Windows 2000/XP/2003 Server/Vista, you must have Administrator rights. Remember that all programs must be closed before you start with the installation.



In the License Agreement window agree to the license agreements and click on the button [Continue]. In the next step select your USB type of connection.

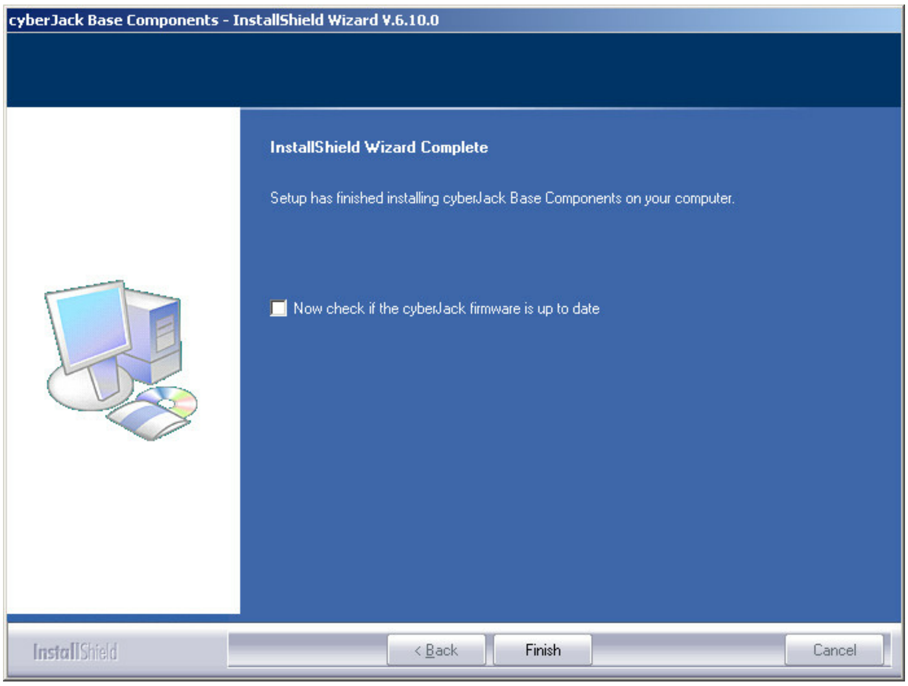


Select the driver for your chip card reader by clicking on the relevant box. Click on [Continue].



Click on [Continue] if you want to install the program in the displayed folder. If you wish to install the files in a different folder, click on [Change] and select the desired path. Then select [Install] and installation of the drivers begins.

When installation is completed the PC must be rebooted in order to activate the installed drivers.



In the Windows Start menu a new REINER SCT cyberJack folder is created with the menu items: cyberJack Device Manager, function test, REINER SCT on the Internet, Support Query and Update ACS components.

4.3 How to install drivers under Linux

This RFID chip card reader is currently supported by the following operating systems: openSuSE-11.1-i586, openSuSE-11-1-x86_64, openSuSE-11-2-i586, openSuSE-11-2-x86_64, debian-500-i386, debian-500-amd64, ubuntu-9.04-desktop-i386, ubuntu-9.04-desktop-amd64, ubuntu-10.04.1-desktop-i386,ubuntu-10.04.1-desktop-amd64.

4.3.1 Linux.deb

4.3.1.1 Description for ubuntu

To install the driver for the cyber***Jack***® **RFID universal** you need an Internet connection.
Do not plug in the chip card reader yet!

Installation of the driver for the cyber***Jack***® **RFID universal** is divided into two steps:

a) How to install the PCSCD driver and its dependencies
b) Installation of the up-to-date driver for the cyber***Jack***® **RFID universal**

How to proceed:
1. Please first install the PCSCD driver with the aid of the package management system of your distribution.
2. Then download the up-to-date driver to match your distribution and your processor at www.reiner-sct.com/treiber .
3. Install this driver by means of a double click.
4. Add your user of the cyberjack unit. To do so use the command *usermod –aG cyberjack "username“* in the terminal input.
5. Please reboot.
6. Installation of the driver is now complete. Now you can plug the cyber***Jack***® **RFID universal** into a USB port on your computer and use it.

Functions test: Place the login***card*** or the new electronic ID card on the connected chip card reader. If the installation is correct the green light-emitting diode (LED) on the chip card reader lights up.

Note: To use the cyber***Jack***® **RFID universal** you require an application program and an RFID chip card or the new electronic ID card.

4.3.1.2 Description for debian

To install the driver for the cyber***Jack***® **RFID universal** you need an Internet connection.
Do not plug in the chip card reader yet!

Installation of the driver for the cyber***Jack***® **RFID universal** is divided into two steps:

a) How to install the PCSCD driver and its dependencies
b) Installation of the up-to-date driver for the cyber***Jack***® **RFID universal**

How to proceed:
1. Please first install the PCSCD driver with the aid of the package management system of your distribution.
2. Then download the up-to-date driver to match your distribution and your processor at www.reiner-sct.com/treiber .
3. Install the driver by means of the following command in the terminal input.
   Command: *dpkg -i (file name).deb*
4. Add your user of the cyberjack unit. To do so use the command *usermod –aG cyberjack "username"* in the terminal input.

Please note that these commands must be executed as root commands.

5. Please reboot.
6. Installation of the driver is now complete. Now you can plug the cyber***Jack***® **RFID universal** into a USB port on your computer and use it.

Functions test: Place the login***card*** or the new electronic ID card on the connected chip card reader. If the installation is correct the green light-emitting diode (LED) on the chip card reader lights up.

Note: To use the cyber***Jack***® **RFID universal** you require an application program and an RFID chip card or the new electronic ID card.

4.3.2 Linux.rpm

Description for SuSE Linux

To install the driver for the cyber***Jack***® **RFID universal** you need an Internet connection.
Do not plug in the chip card reader yet!

Installation of the driver for the cyber***Jack***® **RFID universal** is divided into two steps:

a) Installation of the PCSCD driver and its dependencies
b) Installation of the up-to-date driver for the cyber***Jack***® **RFID universal**

How to proceed:
1. Please first install the PCSCD driver with the aid of the package management system of your distribution.
2. Then download the up-to-date driver to match your distribution and your processor at www.reiner-sct.com/treiber .
3. Install this driver by means of a double click.
4. Please reboot.
5. Installation of the driver is now complete. Now you can plug the cyber***Jack***® **RFID universal** into a USB port on your computer and use it.

Functions test: Place the login***card*** or the new electronic ID card on the connected chip card reader. If the installation is correct the green light-emitting diode (LED) on the chip card reader lights up.

Note: To use the cyber***Jack***® **RFID universal** you require an application program and an RFID chip card or the new electronic ID card.

4.4 Driver installation under Mac

This RFID chip card reader is currently supported by MAC OS X. You will find more extensive information here.

With this function the cyber***Jack***® **RFID universal** is connected to the USB port of your computer or to a USB hub. **Before you plug in the RFID chip card reader please read the following information without fail!**

A driver installation is imperative for the cyber***Jack***® **RFID universal**.

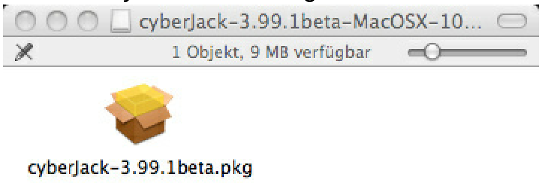
How to proceed with the driver installation for the operating system is to be found in the following chapter:

- Mac OS X 19

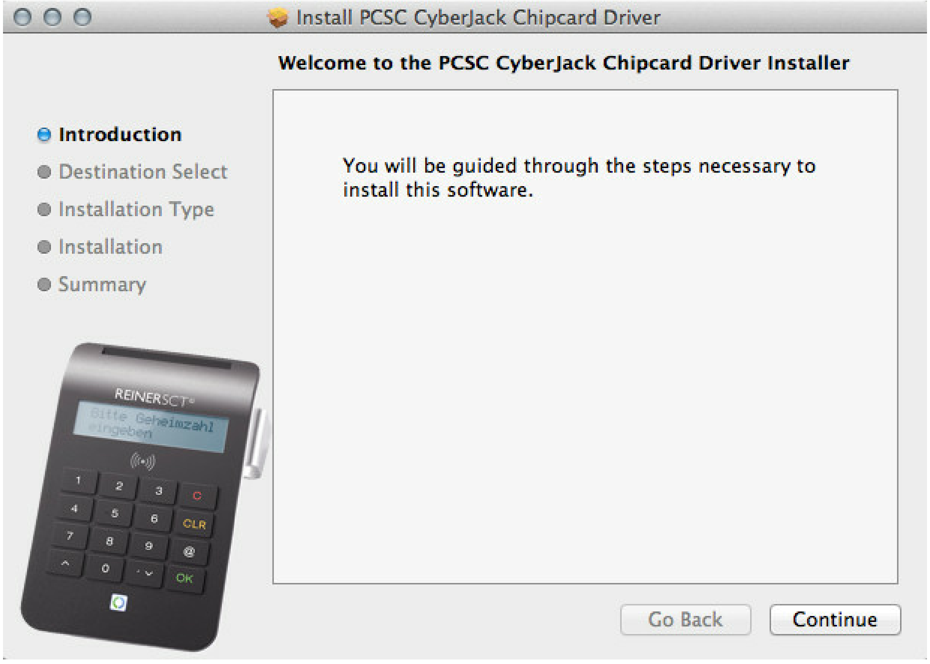
4.4.1 Mac OS X

To install the driver for the cyber***Jack***® **RFID universal** you need an Internet connection.
Do not plug in the chip card reader yet!

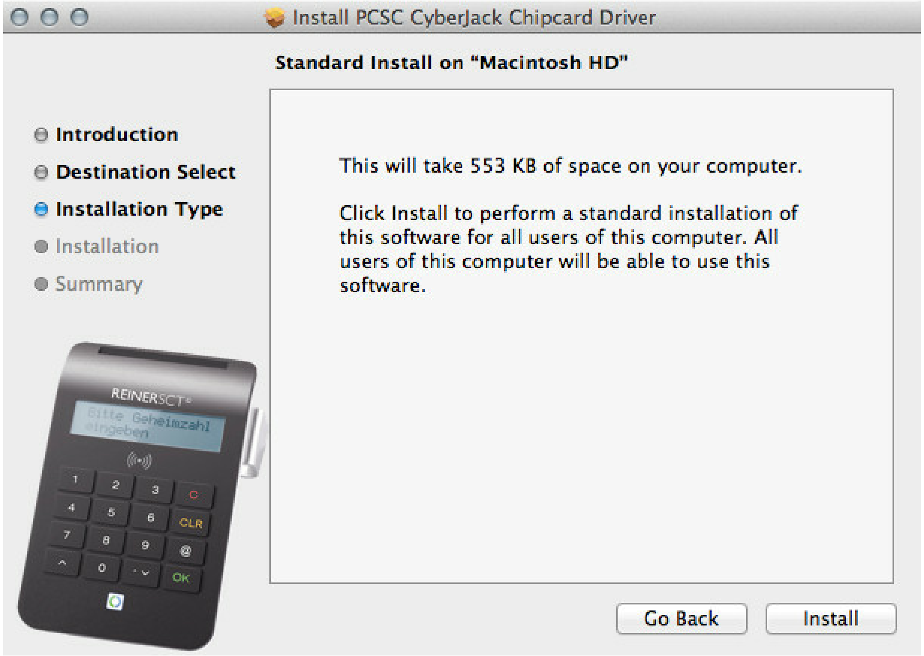
Download the driver for the cyber***Jack***® **RFID universal** at www.reiner-sct.com/treiber and execute the driver file by double-clicking it. You will now be guided through the installation.



Click on the "**Continue**" button to start the driver installation.

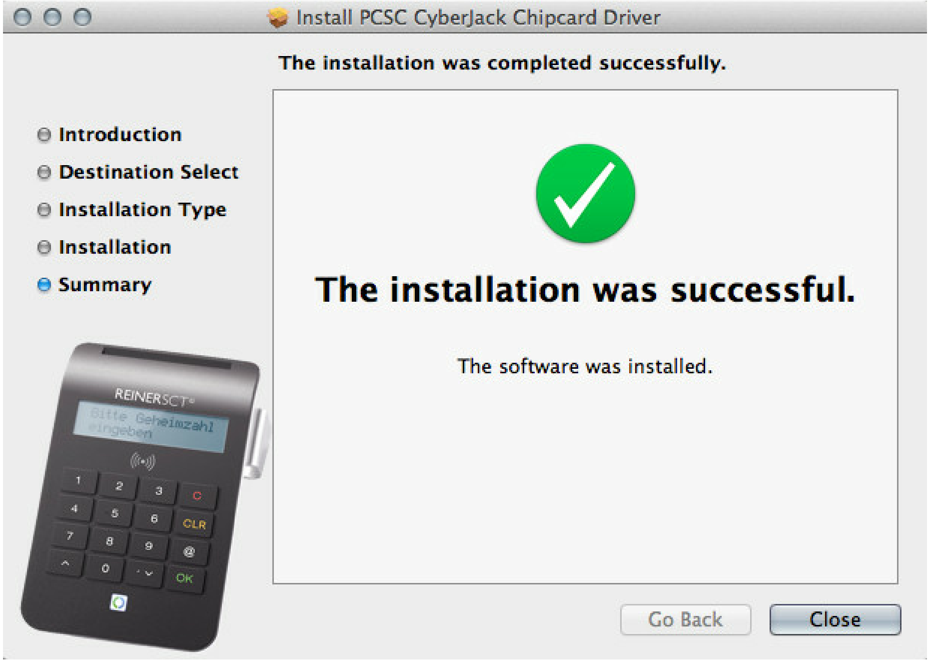


Click on the "**Install" button**".



By inputting your user name and password you permit the driver to be installed. Please note that the user must possess the rights for this.

Installation of the driver is now complete.



Now you can plug the cyber***Jack***® **RFID universal** into a USB port on your computer and use it.

Functions test: Place the login***card*** or the new electronic ID card on the connected chip card reader. If the installation is correct the green light-emitting diode (LED) on the chip card reader lights up.

Note: To use the cyber***Jack***® **RFID universal** you require an application program and an RFID chip card or the new electronic ID card.

5 Safety notes

Organisational safety measures:

- Make sure that unauthorised persons do not obtain access to the card reader. The reader must be operated such that abuse is excluded.
- Make sure that the PC possesses suitable protective measures (such as a virus scanner, firewall) and manipulation by unauthorised persons is prevented.
- Each time the chip card reader is used, take care to check that the chip card reader and the security features (e.g. seal) are intact.
- Pay regard to the status of the device which is displayed to you via the LED (refer to the LED functions chapter 24).
- Follow the screens on the display through the process of secure PIN input (the so-called PIN dialog, refer to the Secure PIN input function chapter 7).

The safety of small children

The devices and accessories may contain small parts. Keep these out of reach for small children.

General safety note

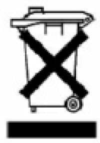
Do not put any foreign bodies in the card slot. On no account should you throw the device into a fire.

Care and maintenance

Your device was developed and manufactured with great care and should also be treated with care. The following recommendations are to help you to ensure the long-term operation of your cyber***Jack***® **RFID**
:

- Do not use or keep the device industy or dirty environments. The movable parts and electronic components may be damaged.
- Do not keep the device in hot environments. High temperatures can shorten the service life of electronic devices and distort certain plastics or make them melt.
- Do not keep the device in cold environments. When the device thereafter returns to its normal temperature moisture may form inside it and damage the electronic circuits.
- Do not drop the device or expose it to blows or shocks and do not shake it. If handled roughly the electronic circuits and mechanical fines inside the device may be damaged.
- Refrain from using any harsh chemicals, cleaning solutions or strong cleaning agents to clean the device.
- Do not paint the device. The paint can make the moving parts stick together and prevent it from working properly.
- Clean the display and housing with a soft, clean and dry cloth only.
- If a device is not working properly bring it to your institute or back to the specialist dealer where you bought it.

Disposal of old electronic devices



This symbol on the product, or its packaging, points out that it must not be disposed of with the domestic waste. Instead bring it to a collection point for electronic devices which passes the product on for recycling. By disposing of this product correctly you are avoiding potential harm to the environment and health which can arise from its incorrect disposal. Besides, recycling materials spares natural resources. Detailed information about recycling this product can be obtained from the responsible authority in your town or community or from waste disposal companies.

6 Support

Help in case of faults

In case of faults which cannot be remedied by restarting your cyber***Jack***® **RFID** (see chapter 4), please contact our Service department via our homepage at
www.reiner-sct.com

Service

You have purchased a high quality REINER SCT product which is subject to strict quality control. If problems should occur or you have questions regarding how to opeate the device you can always send a support query to our Service department at
support@reiner-sct.com .

Warranty

REINER SCT gives a 60-month warranty for the material and manufacture of the chip card reader from the time it is handed over. The purchaser is entitled to rectification of defects. Instead of rectification, REINER SCT can supply replacement devices. Replaced devices become the property of REINER SCT.
The warranty lapses if the purchaser or an unauthorised third party interferes with it. Damage caused by improper treatment, operation, storage and force majeure or other external influences do not come under the warranty.

Interface information for developers

Developers who want to integrate the cyber***Jack***® **RFID** chip card reader into their applications are welcome to contact support@reiner-sct.com concerning their questions.

7 Technical references

7.1 LED functions

Light-emitting diodes (LED)

The cyber***Jack***® **RFID universal** is equipped with a yellow and a dual LED. The dual LED can assume the colours blue and green. Green signifies interaction with a contact-type chip card and blue indicates interaction with a contactless chip card.

The function of the dual LED can be checked by first inserting a contact-type card into the chip card reader (green LED flashes briefly) and then inserting a contactless card into the chip card reader (blue LED flashes briefly).

The function of the yellow LED can be checked after plugging in the USB plug. While the revision number is indicated in the chip card reader display it must flash in yellow.

If this is not the case, the device is defective. Please contact our Support at support@reiner-sct.com .

The light-emitting diodes (LED) can be in the following states:

Yellow LED	Green dual LED	Green dual LED	Significance
flashes steadily		shines permanently	Secure PIN input mode with contactless cards; displayed text is authentic.
flashes steadily	shines permanently		Secure PIN input mode with contact-type cards; displayed text is authentic.
flashes steadily			The cyber***Jack***® **RFID universal** performs a firmware update or shows the text authentically in the display.
flashes steadily		flashes steadily	If the yellow LED and blue dual LED are flashing in synchrony, the chip card reader is in an endless loop in which the only thing that can take place is the flashing of the LED either caused intentionally or due to technical failure. No other functions are then feasible. The chip card reader can only be restarted by removing the card and inserting it again. Please unplug the chip card reader and then plug it in again after approx. 3 seconds. If the fault persists, please contact our Support at support@reiner-sct.com .
	shines permanently		The interface to the contact-type chip card is activated (operational status).
	flashes		Within the last 3 seconds card communication has taken place with the contact-type chip card.
		shines permanently	The interface to the contactless chip card is activated (operational status).
		flashes	Within the last 3 seconds card communication has taken place with the contactless chip card.

The dual LED cannot shine in both colours simultaneously or alternately because only one interface at a time is active.

7.2 Technical operating environment

The technical environment for the cyber***Jack***® **RFID universal** comprises a PC equipped with a USB interface and drivers to which the cyber***Jack***® **RFID universal** is connected.

Contact-type chip card interface

The cyber***Jack***® **RFID universal** chip card reader processes chip cards the body of which is physically specified in the ISO standards 7810, 7813 and 7816, part 1. The contacting unit of the chip card reader contacts electric contacts of a microprocessor applied to the body of the card. Its position and electrical assignment is defined in the ISO Standard 7816 part 2. The cyber***Jack***® **RFID universal** chip card readers process both processor cards and the asynchronous communication protocols T=0 and T=1, and memory cards with the synchronous 2-wire, 3-wire and I²C-bus communication protocols. These communication protocols are specified in the ISO 7816 part 3 (asynchronous) and in manufacturer-specific data sheets (synchronous).

Contactless chip card interface

The chip card reader support protocol types A and B according to ISO/IEC 14443. Operation of contactless chip cards by the chip card reader takes place in compliance with the ISO/IEC 14443-2, ISO/IEC 14443-3 and ISO/IEC 14443-4 standards.

Secure PIN

The secure PIN input is performed via the communication protocols specified in ISO 7816 part 3. During the Secure PIN input mode the command filter security function ensures that only approved commands are transmitted to the chip card. All other commands to the chip card are blocked by the chip card reader (c.f. chapter on Security functions 25).

7.3 Security functions

Secure PIN input is one of the most important security functions of a chip card reader from security class 2 upwards. Secure PIN input is feasible with both a contact-type and a contactless chip card. To ensure that the PIN is not stored in the chip card reader special security functions have been implemented in the cyber***Jack***® **RFID universal.** The following security functions have been implemented in the cyber***Jack***® **RFID universal**:

Separation of applications

The cyber***Jack***® **RFID universal** prevents the applications from influencing one another by separating them. The commands received from the PC are passed on to the relevant application which then fully processes them. Only when the commands have been processed does the PC accept new commands.

Module update

It is possible to add new modules to the chip card reader with the aid of the Device Manager (refer to the Device Manager chapter 3). These new modules (kernel, application) can be acquired from the REINER SCT homepage (www.reiner-sct.com). In order to upload a new module into the chip card reader the origin of the module is checked by the chip card reader itself as an important security function. The chip card reader only accepts modules which are electronically signed by REINER SCT by means of the RSA method. Each time before uploading a new module the chip card reader always performs a signature check. Modules can be uploaded and updated individually, or all together. Uploaded modules do not influence the functionality of the other modules. It is impossible to store a module in the chip card reader which has not been electronically signed by REINER SCT. REINER SCT provides only evaluated versions. It is impossible to update the cyber***Jack***® **RFID universal** to an older version.

Communication separation

After activating the "Secure PIN input" mode by an application, the cyber***Jack***® **RFID universal** interrupts the communication with the PC, switches the yellow LED into the flashing mode and the corresponding dual LED (green for contact-type, blue for contactless chip cards). In secure PIN input the cyber***Jack***® **RFID universal** records all keyboard inputs and passes them on exclusively to the card. Before communication separation is released these data are deleted by another security function °(reprocessing).

The interruption of communication with the PC is software-controlled by means of a lock which ensures that in the Secure PIN input mode no data are transmitted from the memory (PIN data). Only log information is transmitted to the PC which is always transferred directly to the hardware interface in the form of constants.
Should the chip card reader indeed switch to the routine for PC communication owing to a malfunction, the Secure PIN input mode is identified there and the switch made to the "Stop" security routine. In this routine the chip card reader is reinitialised, the entire Interrupt system is switched off and the yellow LED flashes in synchrony with the blue Duo LED. The only way to exit is by unplugging the chip card reader and plugging it in again.
Communication separation cannot be influenced from the outside via interfaces.

Reprocessing

The reprocessing security function reprocesses the area of the memory in which the PIN data are buffered during the Secure PIN input mode (the storage locations of the PIN data are overwritten with zeros). This prevents PIN data in the temporary memory from being read out.
The area of the memory is overwritten with zeros before communication with the PC is restored (after the secure PIN input). This takes place both after the PIN data have been successfully transmitted to the contact-type signature-creation unit (chip card) of if the PIN input is cancelled by the user or by a timeout.
During Secure PIN input, if an error occurs followed by a system start the relevant memory area is reinitialised thus also deleting any PIN data present.
By overwriting the memory locations of the PIN data with zeros the cyber***Jack***® **RFID universal** guarantees that these data are no longer contained in the memory areas and therefore - when the Secure PIN input is finished - they cannot be read out.

Reinitialisation

The reinitialisation security function reinitialises the memory of the cyber***Jack***® **RFID universal** . This is effected by overwriting the entire RAM with zeros. The one exception: a few bytes for the stack memory and a few bytes for saving the status quo of the USB system. These are for the controller function and therefore absolutely necessary for the system.
The security function is applied when the cyber***Jack***® **RFID universal** is started by inserting the chip card reader into the PC, after a watchdog reset or after a control reset.

A watchdog reset takes place if faults - which have been caused intentionally or owing to technical failure - occur in the functional process of the cyber***Jack***® **RFID universal** (especially due to commands which cannot be interpreted) the watchdog timer is not reset within a certain time span and the watchdog therefore triggers a controller reset.
After a reset by the watchdog the chip card reader is subsequently stopped and the yellow LED and the blue Duo LED flash in synchrony.
When a normal start takes place the currently valid version number of the active firmware is shown in the display of the chip card reader. The authenticity of the version displayed is indicated to the user by the flashing yellow LED.

Command filter

With this function the cyber***Jack***® **RFID universal** prevents commands from being forwarded to the chip card which are suitable for saving the PIN data on the chip card or for manipulating them.
Therefore within the "Secure PIN input" mode only those commands are forwarded to the chip card which can be used for authentication purposes.
These are exclusively:

- VERIFY
- CHANGE REFERENCE DATA
- DISABLE VERIFICATION REQUIREMENT
- ENABLE VERIFICATION REQUIREMENT
- RESET RETRY COUNTER

All other commands to the chip card are blocked by the chip card reader.

Released encryption methods

Released encryption methods are used for encrypted data communication and for secure downloading (module update).

An AES-based solution is used as a random number generator. The generator complies with the class K3 according AIS 20 with the high mechanism strength.

Terminal and passive authentication

The terminal and passive authentication for the new ID card-QES is carried out with the certified chip in the security module present in the reader and the certificates from the certificate memory. The identification data of the chip (password) are stored, tamper-proof, in the chip card reader memory and are used as part of initialisation for authentication vis-à-vis the chip.

MPU rules

To ensure that the firmware does not jump into a non-verified code, the MPU rules (access rules for the memory) is implemented in the cyber***Jack***® **RFID universal** . This means that the chip card reader never accesses memory areas not permitted by Reiner SCT.

7.4 Regulatory Notes

Radiofrequency radiation exposure Information

The radiated output power of the device is far below the FCC radio frequency exposure limits. Nevertheless, the device shall be used in such a manner that the potential for human contact during normal operation is minimized.
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
This device complies with Part 15 of the FCC Rules [and with RSS-210 of Industry Canada].

Operation is subject to the following two conditions:
1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications made to this equipment not expressly approved by (manufacturer name) may void the FCC authorization to operate this equipment.

8 Declaration of Conformity

8.1 cyberJack RFID universal

© 2012 REINER Kartengeräte GmbH & Co. KG

REINERSCT

DECLARATION OF CONFORMITY

FCC ID: Q4K-2718800

The manufacturer: Reiner Kartengeräte GmbH & Co. KG
Goethestrasse 14
78120 Furtwangen

declares, in sole responsibility, that the equipment:

cyber*Jack*® RFID universal

(Name, type or model, lot -, batch - or serial number, if possible origin and quantity)

referred to in this declaration, are in accordance with the R&TTE guidelines/ standards 1999/5/EG listed below including all relevant changes of the European Parliament and of the EEC - Council from 09. March 1999.

The following standards / regulations were utilised to test the product for EMC conformity:

EMV as per Schuhwerk-EMV-labority-no.: 2011024

EN 301489-1 V1.8.1 : 2008

RF as per Schuhwerk-EMV--labority-no.: 2011025

EN 300 330-2 : 2010, frequency 13.56 MHz

EN 60950-1 : 2006

(Title and/or number, as well as date of issue of the standard(s) or other standards documents)

Above named company has the following Technical Documentation ready for examination:

- User´s Manual according to regulations
- Plans
- Description of the Quality Control System
- Other Technical Documentation such as:
  Service manual

Internal : Consideration of the REINER quality control system manual

Corporate Reference: The entire technical CE/ GS-Documentation is filed under ZN 20510500000

Furtwangen, 23th October 2012
(Place and date of issue)

Klaus Bechtold
Managing Director
(Name and signature and position of undersigner)

REINER SCT PDM
PC-20710500-000-1 KFT
DECLARATION OF CONFORMITY cj_RFID_universal

Index

- D -

Deactivate
  RFID 13

Declaration of Conformity 28

Device Manager 3

Driver installation
  Debian 18
  Linux .rpm 18
  MAC 19
  Ubuntu 17
  Windows 14

- F -

Firmware download 25

- L -

LED
  function 24

- P -

Product seal 2

- S -

Safety notes 22

Seal 2

Secure changing of the PIN 7

Secure PIN input 7, 25

Support
  Service 23
  Warranty 23

- U -

Upacking and installation 2

REINER Kartengeräte GmbH & Co. KG

Goethestrasse 14
78120 Furtwangen
Germany
Phone: +49 (7723) 5056-0
Telefax: +49 (7723) 5056-778
E-Mail: sales@reiner-sct.com
Internet: www.reiner-sct.com